Lecture 8 – Open-source Software Security

[COSE451] Software Security

Instructor: Seunghoon Woo

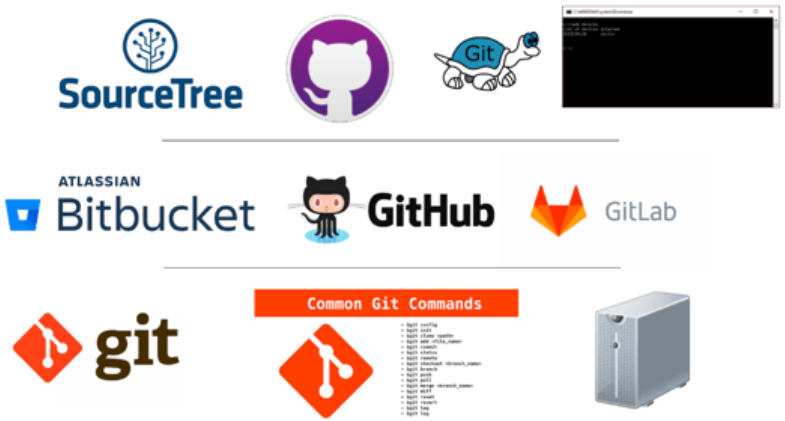
Spring 2024

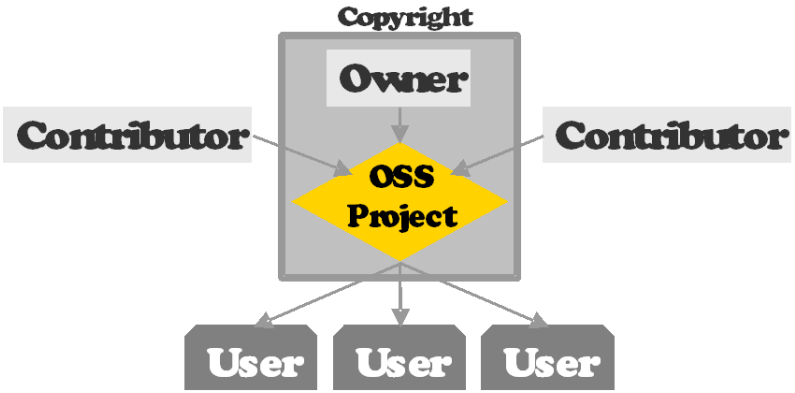
Overview

- **Open-source software & Licenses**
- **Vulnerabilities in OSS**

Open-source Software (OSS)

- **Open-source Software (OSS)**
  - Software that is distributed with its source code, making it available for use, modification, and distribution, and with a license for rules to use





https://www.cobalt.io/blog/risks-of-open-source-software

Open-source Software (OSS)

- **OSS reuse**
  - OSS can be used for business innovation and open collaboration, in addition to faster implementation than competitors (not for incompetent copycats)
  - E.g., Python OSS usage

Overview

96%

of the total codebases **contained** open source

77%

of all code in the total codebases **originated** from open source

Open-source Software (OSS)

- **OSS is always free and there are no restrictions on its use?**

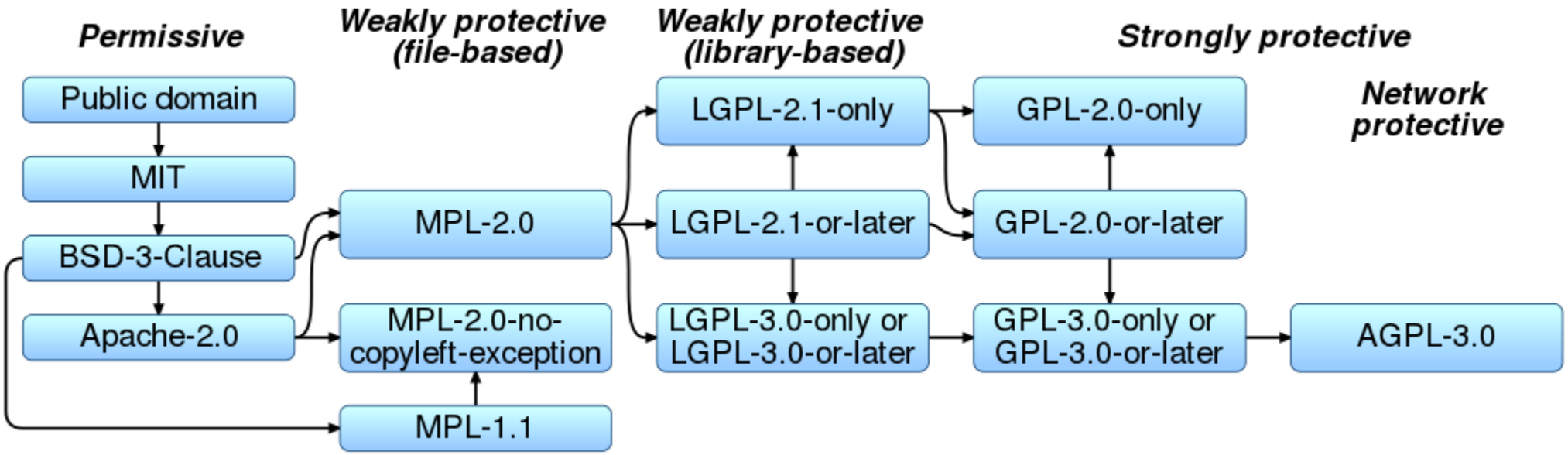
Open-source Software (OSS)

- **OSS is always free and there are no restrictions on its use?**
  - NO!
  - It is free as long as we comply with the license!

Open-source Software (OSS)

- **Types of Licenses**
  - Various types of licenses, ranging from more permissive to more restrictive
  - Some of the most common ones include
    - MIT License
    - GNU General Public License (GPL)
    - Apache License
    - BSD License
  - Each license has its own terms and conditions that state how the software can be used and distributed

Open-source Software (OSS)



https://en.wikipedia.org/wiki/License_compatibility#/media/File:Floss-license-slide-image.svg

Open-source Software (OSS)

- **Types of Licenses**

License	Available for free	Distribution allowed	Source code available	Source code can be modified	Obligation to re-disclose derivative works (2차 저작물 재공개 의무)	Can be combined with proprietary SW
GPL	O	O	O	O	O	X
LGPL	O	O	O	O	O	O
MPL	O	O	O	O	O	O
BSD	O	O	O	O	X	O
Apache	O	O	O	O	X	O

Open-source Software (OSS)

- **Types of Licenses**

"The GNU General Public License does not permit incorporating your program into proprietary programs"

License	Available for free	Distribution allowed	Source code available	Source code can be modified	Obligation to re-disclose derivative works (2차 저작물 재공개 의무)	Can be combined with proprietary SW
GPL	O	O	O	O	O	X
LGPL	O	O	O	O	O	O
MPL	O	O	O	O	O	O
BSD	O	O	O	O	X	O
Apache	O	O	O	O	X	O

Open-source Software (OSS)

"You must make the source code for any of your changes available under MPL, but you can combine the MPL software with proprietary code, as long as you keep the MPL code in separate files"

- **Types of Licenses**

License	Available for free	Distribution allowed	Source code available	Source code can be modified	Obligation to re-disclose derivative works (2차 저작물 재공개 의무)	Can be combined with proprietary SW
GPL	O	O	O	O	O	X
LGPL	O	O	O	O	O	O
MPL	O	O	O	O	O	O
BSD	O	O	O	O	X	O
Apache	O	O	O	O	X	O

Open-source Software (OSS)

- **Types of Licenses: very relaxed license**
  - Beerware

```
/*
 * ----------------------------------------------------------------------
 * "THE BEER-WARE LICENSE" (Revision 42):
 * <phk@FreeBSD.ORG> wrote this file.  As long as you retain this notice you
 * can do whatever you want with this stuff. If we meet some day, and you think
 * this stuff is worth it, you can buy me a beer in return.   Poul-Henning Kamp
 * ----------------------------------------------------------------------
 */
```

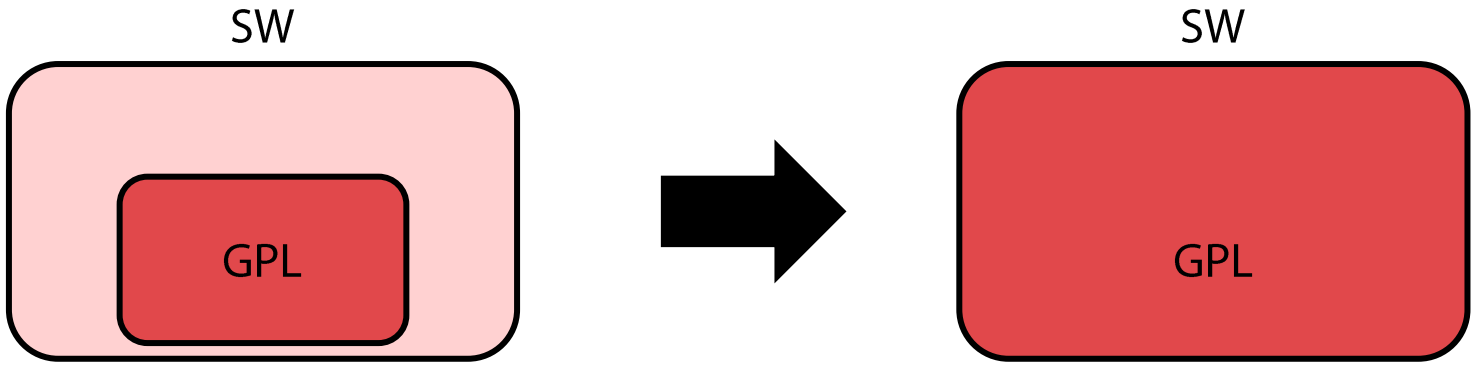
Open-source Software (OSS)

- **Types of Licenses: very strict license GPL**
  - Modified programs must also have their source code publicly distributed
  - Modified computer programs must also obtain the same license
    - I.e., the GPL license must be applied
  - Representative OSS: Linux Kernel

```
                    GNU GENERAL PUBLIC LICENSE
                       Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
                       51 Franklin St, Fifth Floor, Boston, MA  02110-1301  USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.
```

Open-source Software (OSS)

- **Types of Licenses: very strict license GPL**



Open-source Software (OSS)

- **License compatibility (compatibility issue)**
  - The issue of conflicting license between each OSS when developing a new program using multiple open-source projects
    - Conflict between proprietary and open source licenses
    - Conflicts between open source licenses
  - Example
    - GPLv2 and GPLv3 / MPL and GPL
      - Each open source must be distributed under the corresponding license when using it

Overview

96%
of the total codebases **contained** open source

53%
of the total codebases **contained license conflicts**

77%
of all code in the total codebases **originated** from open source

31%
of the total codebases contained open source with **no license** or a **custom license**

Open-source Software (OSS)

- **License compatibility (compatibility issue)**
  - How to resolve it?
    - Separate design to ensure that the scope of derivative works does not overlap
    - Replacement with other licensed SW that does not cause license conflicts
      - E.g., If a commercial version of open source SW exists, replace it with the commercial version
    - In-house development of open source SW to avoid licensing conflicts
  - There is no clear guide on compatibility between licenses, thus it is necessary to carefully read the provisions of each license when using multiple OSS

Open-source Software (OSS)

- **License violation**
  - Hancom case
    - Hancom software has been using GhostScript* OSS since 2013
    - GhostScript utilizes the AGPL license (an extended version of the GPL)

Platform/License	GNU Affero General Public License
Ghostscript 10.03.0 for Windows (32 bit)	Ghostscript AGPL Release

*GhostScript: an interpreter for the PostScript language and PDF file

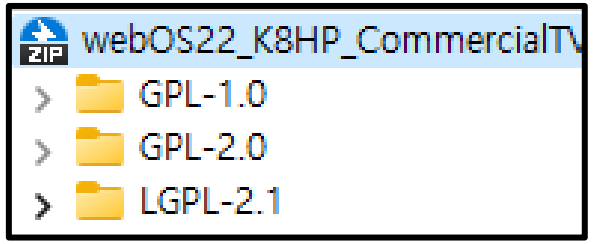
Open-source Software (OSS)

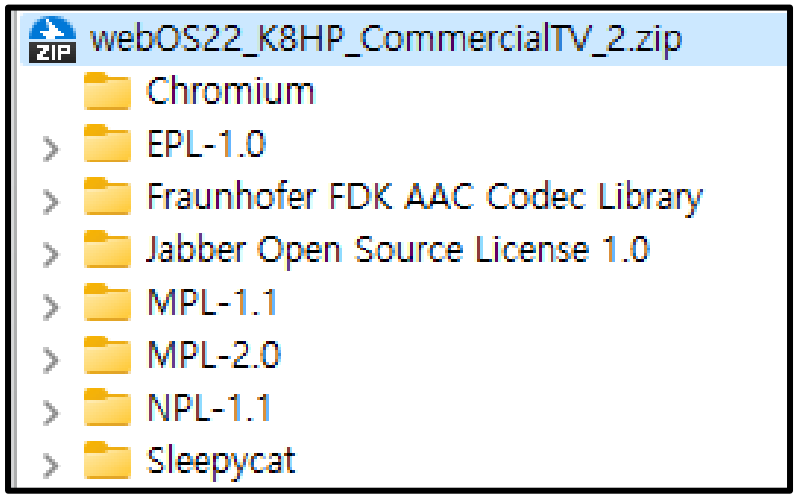
- **License violation**
  - Hancom case
    - Hancom software has been using GhostScript* OSS since 2013
    - GhostScript utilizes the AGPL license (an extended version of the GPL)
    - Hancom had two choices
      1. Pay money to hide the source code
      2. Make the code public and notify that they are using GPL-licensed GhostScript
    - However, Hancom does not pay and distribute the software under the GPL
      - After 2016, the code was removed at GhostScript's request

*GhostScript: an interpreter for the PostScript language and PDF file

Open-source Software (OSS)

- **Example: LG Smart TV (15LN766A0UB)**

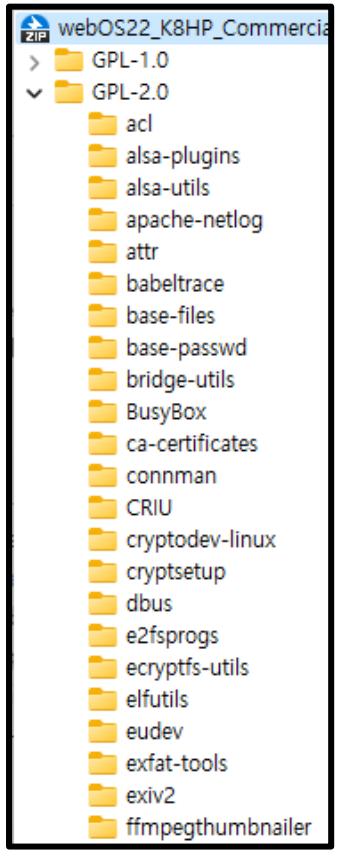


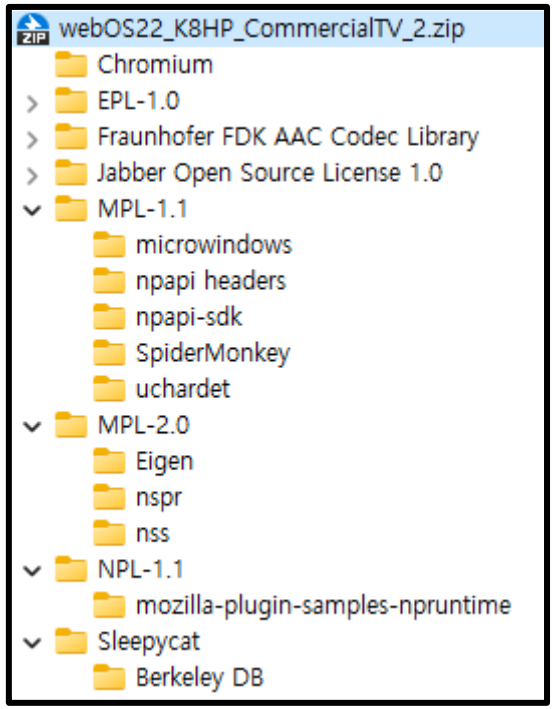


Separate the MPL-licensed part from the GPL-licensed part and keep each part independent

Open-source Software (OSS)

- **Example: LG Smart TV (15LN766A0UB)**





Open-source Software (OSS)

- **Is open-source software safe?**

Open-source Software (OSS)

- **Is open-source software safe?**
  - (In general) YES!
  - Code transparency ensures safety
  - Numerous third eyes detect and report security vulnerabilities

Open-source Software (OSS)

WOOSEUNGHOON commented on Jul 30, 2019

Godot version:
v3.1.1-stable_win 64 binary

Issue description:
Hi,
I found a unpatched CVE-2017-0700 vulnerability in **godot/thirdparty/jpeg-compressor/jpgd.cpp**.

The vulnerability was reported as an Android vulnerability in NVD, but in fact,
it was identified as a vulnerability in code in Libgdx.

I found the PoC at https://github.com/ele7enxxh/poc-exp/tree/master/CVE-2017-0700
and confirmed that the program was terminated as soon as I inserted the eval jpg input
into the godot program.

For vulnerability information, please refer to https://nvd.nist.gov/vuln/detail/CVE-2017-0700 and related patch information is found in https://android.googlesource.com/platform/external/libgdx/+/38889ebd9b9c682bd1b64fd251ecd69b504a6155.

Thanks.

+ Add tasklist

akien-mga added bug high priority topic:thirdparty labels on Jul 30, 2019

akien-mga added this to the **3.2** milestone on Jul 30, 2019

[FIX] revisit CVE-2015-8080 vulnerability

unstable (#6875)
7.2.4 ... 6.2-rc1

WOOSEUNGHOON committed on Feb 10, 2020

Showing **1 changed file** with **6 additions** and **4 deletions**.

10 deps/lua/src/lua_struct.c

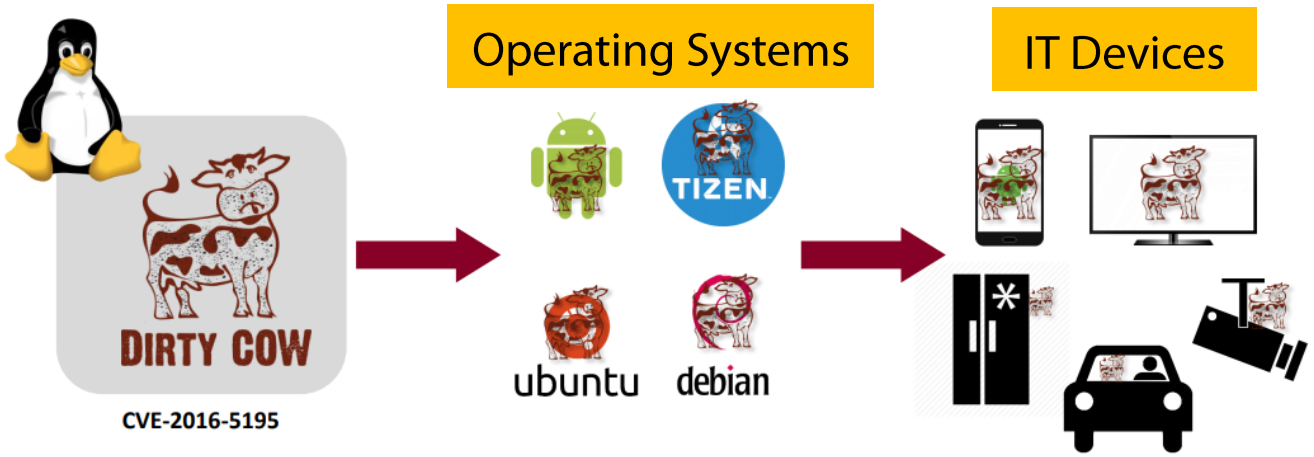
```diff
@@ -89,12 +89,14 @@ typedef struct Header {
 } Header;

 
- static int getnum (const char **fmt, int df) {
+ static int getnum (lua_State *L, const char **fmt, int df) {
   if (!isdigit(**fmt))  /* no number? */
     return df;  /* return default value */
   else {
     int a = 0;
     do {
+      if (a > (INT_MAX / 10) || a * 10 > (INT_MAX - (**fmt - '0')))
+        luaL_error(L, "integral size overflow");
       a = a*10 + *((*fmt)++) - '0';
     } while (isdigit(**fmt));
     return a;
```

Open-source Software (OSS)

- **Is open-source software reuse safe?**

Open-source Software (OSS)

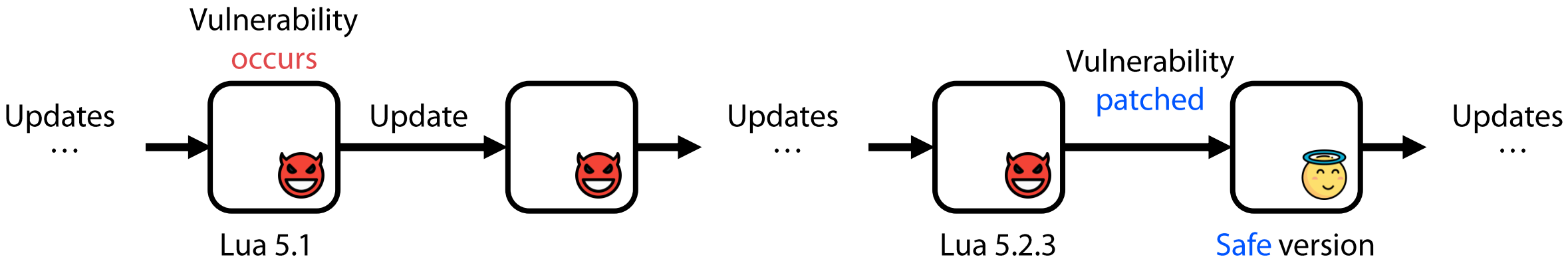
- **Is open-source software reuse safe?**
  - **NO!**
  - Old versions of vulnerable OSS can be reused
  - Even the latest version of OSS may have vulnerabilities in sub-components



Propagation of the Dirty COW vulnerability

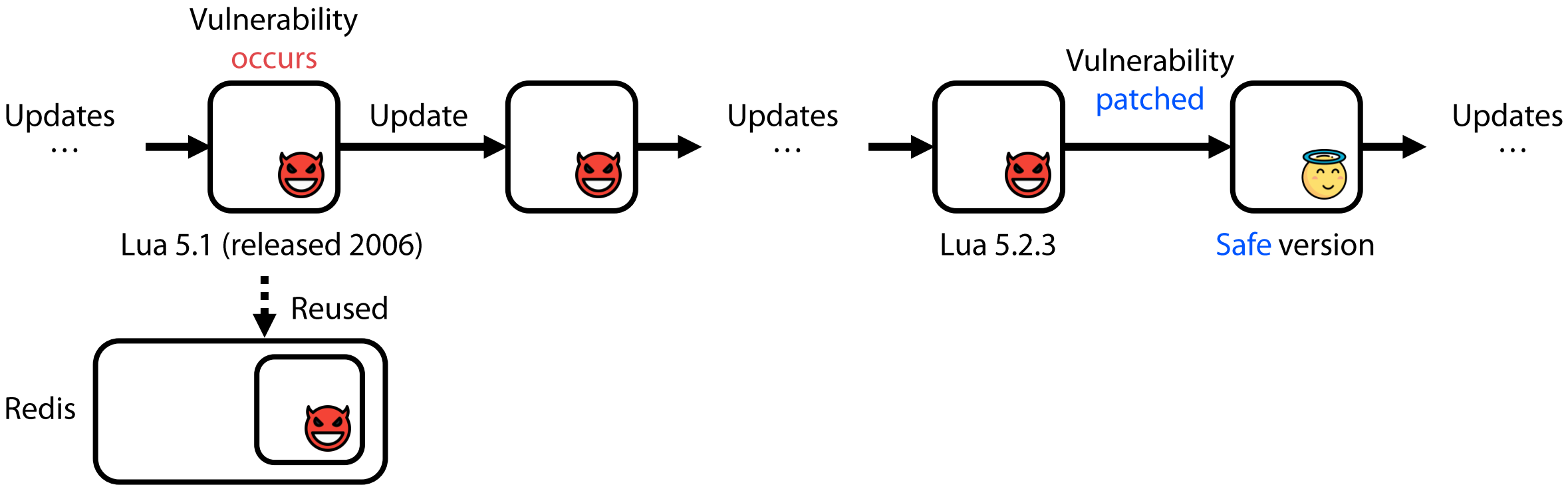
Open-source Software (OSS)

- **Is open-source software reuse safe?**
  - Example: Lua & Redis case



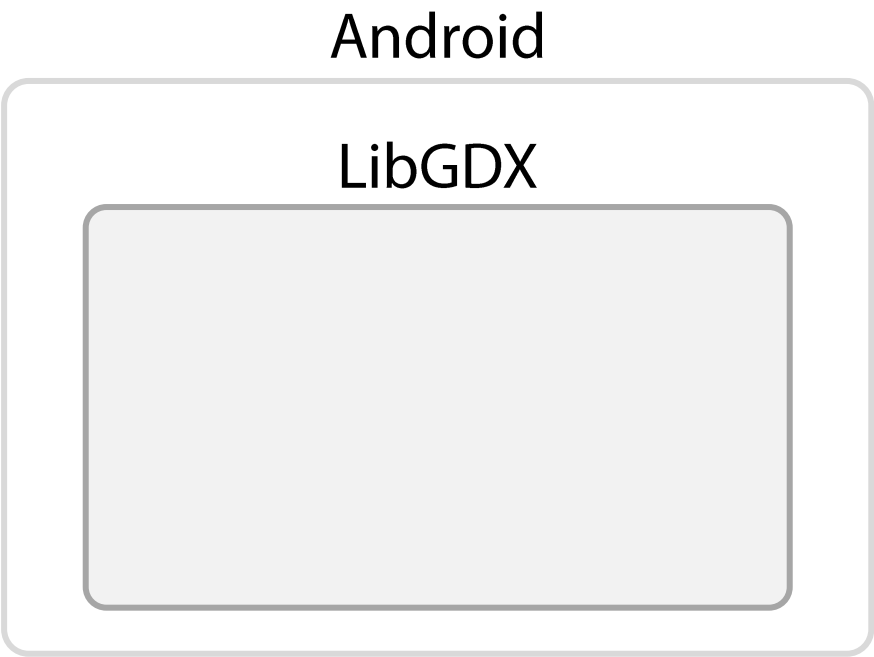
Open-source Software (OSS)

- **Is open-source software reuse safe?**
  - Example: Lua & Redis case



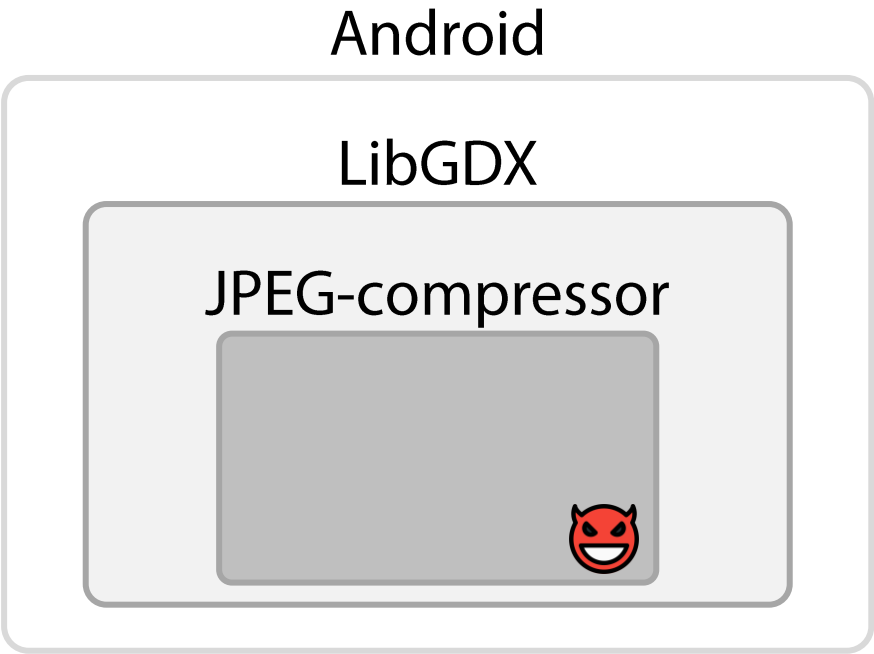
Open-source Software (OSS)

- **Is open-source software reuse safe?**
  - Example: Android case

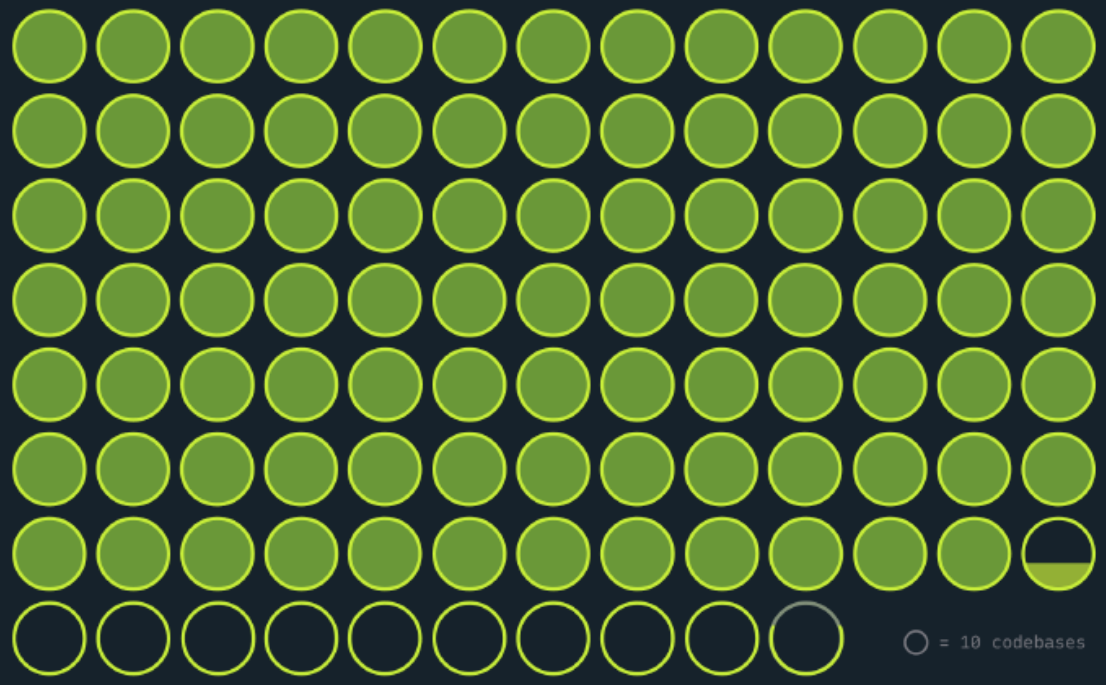


Open-source Software (OSS)

- **Is open-source software reuse safe?**
  - Example: Android case



Overview



1,067 codebases scanned in 2023

936 codebases underwent risk assessments

96% of the total codebases contained open source

53% of the total codebases contained license conflicts

77% of all code in the total codebases originated from open source

31% of the total codebases contained open source with no license or a custom license

10 years

2.8 years

24 months

12 months

14% of the codebases assessed for risk contained vulnerabilities older than 10 years

2.8 years was the mean age of vulnerabilities in the codebases assessed for risk

49% of the codebases assessed for risk had components that had no development activity in the past 24 months

1% of the codebases assessed for risk had components that were at least 12 months behind on code maintainer updates/patches

84% of codebases assessed for risk contained vulnerabilities

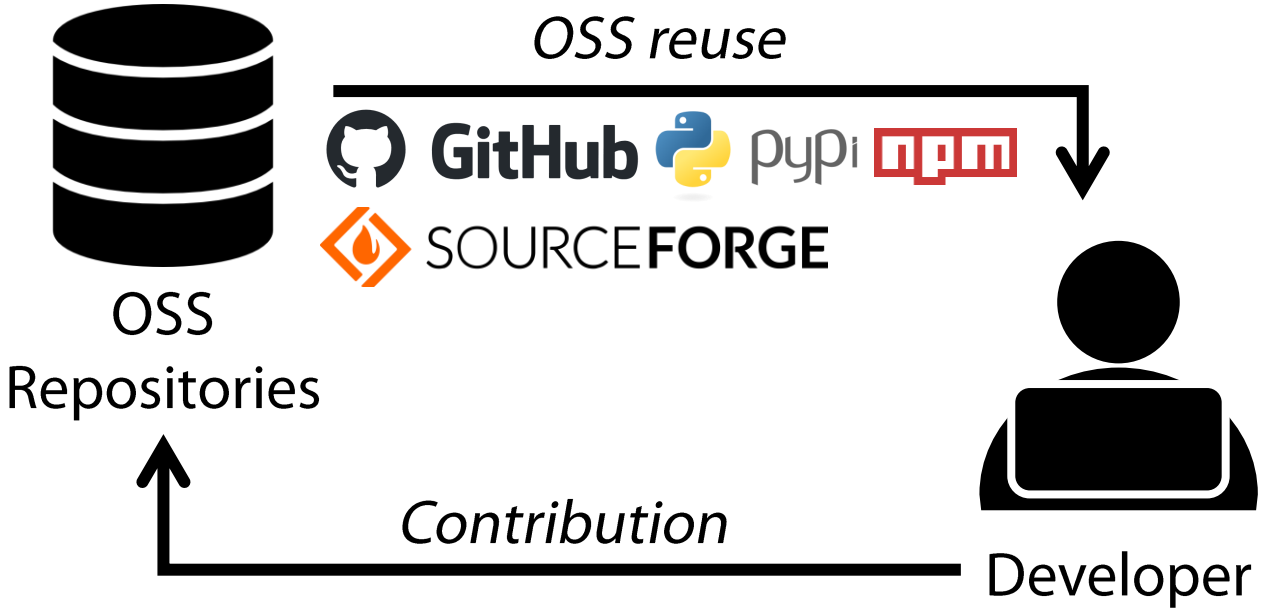
74% of codebases assessed for risk contained high-risk vulnerabilities

91% of the codebases assessed for risk contained components that were 10 versions or more behind the most current version of the component

SYNOPSYS | Open Source Security and Risk Analysis Report 2024 | 4

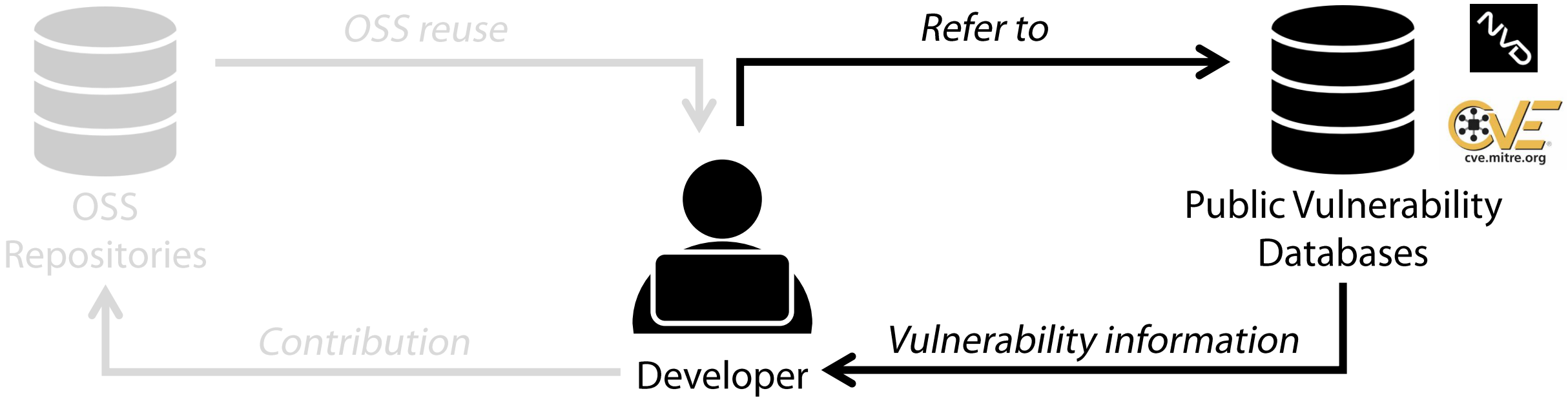
Open-source Software (OSS)

- **A simplified depiction of the OSS reuse process**



Open-source Software (OSS)

- **A simplified depiction of the OSS reuse process**



Next Lecture

- **Security of OSS ecosystem**